UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,901	07/25/2001	Michael L. Wenocur	A-70560/RMA	6591

7590   12/01/2004

FLEHR HOHBACH TEST ALBRITTON & HERBERT, LLP
Suite 3400
Four Embarcadero Center
San Francisco, CA 94111

EXAMINER
POLLACK, MELVIN H

ART UNIT	PAPER NUMBER
2145	

DATE MAILED: 12/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/912,901	WENOCUR ET AL.
	Examiner	Art Unit	
	Melvin H Pollack	2145	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>25 July 2001</u>.
2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-22</u> is/are pending in the application.
   4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) <u>1-22</u> is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on <u>07 September 2001</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.
   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a)☐ All b)☐ Some * c)☐ None of:
   1.☐ Certified copies of the priority documents have been received.
   2.☐ Certified copies of the priority documents have been received in Application No. _____.
   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date <u>1/8/02, 4/5/02</u>.
4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☒ Other: <u>see attached office action</u>.

DETAILED ACTION

Specification

1.   The disclosure is objected to because of the following informalities: the Related

Applications section contains significant gaps in the record, as well as information in need of

updating. The applicant must fill in all of the blanks, and must show which applications have

which status.

        Appropriate correction is required.

Information Disclosure Statement

2.   The information disclosure statements filed 1/8/02 and 4/5/02 fail to comply with 37 CFR

1.98(a)(2), which requires a legible copy of each U.S. and foreign patent; each publication or that

portion which caused it to be listed; and all other information or that portion which caused it to

be listed. It has been placed in the application file, but the information referred to therein has not

been considered. In both cases, the Abrash publication is missing from the file, and thus cannot

be considered.

Claim Rejections - 35 USC § 112

3.   Claim 2 is objected to because of the following informalities: the claim states "network

transport neutral" when it should clearly be "network transport protocol neutral." Appropriate

correction is required.

4.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the
> subject matter which the applicant regards as his invention.

5.   Claim 21 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for

failing to particularly point out and distinctly claim the subject matter which applicant regards as

the invention.

6.   Claim 21 recites the limitation "a Compact Certificate as explained earlier" in claim 2.

There is insufficient antecedent basis for this limitation in the claim. None of the claims mention

a Compact Certificate. Furthermore, claim 21 must be dependent from a claim mentioning a

Compact Certificate and must specify which "earlier" claim is referenced. The claim cannot

reference part of the specification.

Claim Rejections - 35 USC § 102

7.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed
> in the United States before the invention by the applicant for patent or (2) a patent granted on an application for
> patent by another filed in the United States before the invention by the applicant for patent, except that an
> international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this
> subsection of an application filed in the United States only if the international application designated the United
> States and was published under Article 21(2) of such treaty in the English language.

8.   Claims 1-4, 6, 7, 9, 11-20, 22 are rejected under 35 U.S.C. 102(e) as being anticipated by

Geiger et al. (6,463,534).

9.   For claim 2, Geiger teaches (abstract) a hardware architecture neutral and operating

system neutral (col. 4, line 60 – col. 5, line 40; col. 11, lines 10-40) and network transport

protocol neutral (col. 9, lines 20-30) method for secure response session (col. 1, lines 5-col. 2,

line 5) using less software code and network bandwidth than conventional systems (col. 7, lines

40-50), said method comprising the steps of:

a.   Extracting, by a Client (Fig. 1, #11) who is establishing a secure response session to a Entity (Fig. 2, #16 and #17) in order to respond to a message from the Entity (col. 2, lines 55-65), the Entity's public key and matching destination address of the Entity from a trusted source or storage means (col. 6, lines 35-55);

b.   Extracting, by the Client, the Client's public and private key and certificate chain from a trusted source or storage means (col. 17, line 35 – col. 18, line 5);

c.   Using the extracted client public and private key and certificate chain information along with the previously extracted Entity destination address to create a secure session with the Entity using a secure session protocol (col. 13, lines 10-45);

d.   Sending, by the Client, a first Data message after any session setup messages, that contains a Resource Tag that was included in the message received from the Entity to which this client initiated session is a response (col. 9, lines 40-45);

e.   Setting up, by the Entity, the session setup portion of the secure session protocol (col. 6, lines 49-55); and

f.   Verifying, by the Entity, the Client's certificate chain and the Resource Tag that is received in the first Data message from the Client (col. 6, lines 55-65).

10.   Claim 1 is drawn to a software system that effectively describes the limitations of the hardware system drawn in claim 2. It is well known in the art that hardware and software embodiments of the same method and functional limitations are equivalent. Therefore, since claim 2 is rejected, claim 1 is also rejected for the reasons above. A teaching regarding the hardware/software equivalence is available upon request.

11.   For claim 3, Geiger teaches exchanging, between the Client and the Entity, additional

data related to the application that is using the secure response protocol (Fig. 5, #550).

12.   For claim 4, Geiger teaches terminating the session, by either the Client or the Entity, by

closing the underlying network connection (col. 8, lines 20-30).

13.   For claim 6, Geiger teaches that the public key and matching destination address has been

verified previously using a digital signature (verified with a trusted public key) or cryptographic

checksum (verified with a trusted key derived from a Master Key or Session Key or Message

Key) (col. 3, line 50 – col. 4, line 50; col. 5, line 45 – col. 6, line 30).

14.   For claim 7, Geiger teaches that the Entity's public key comprises a RSA or a RSA based

public key (col. 9, lines 60-65; col. 16, lines 55-65).

15.   For claim 9, Geiger teaches that the trusted source or storage means comprises data

selected from the set consisting of a normal conventional e-mail message, a non-secured web

page, a secured web page, and combinations thereof (col. 12, line 55 – col. 13, line 10; col. 14,

line 58 – col. 15, line 15).

16.   For claim 11, Geiger teaches that the trusted storage means comprises data received from

communicating with a Server via a secure session (col. 2, lines 55-57).

17.   For claim 12, Geiger teaches that the Client's keys and certificate chain comprise fixed

values (col. 4, lines 1-50).

18.   For claim 13, Geiger teaches that the Client's keys and certificate chain comprise fixed

values shared by more than one Client system and wherein the Entity authenticates the Client

based on this Resource Tag (col. 10, lines 10-15).

19.   For claim 14, Geiger teaches that the Client's keys and certificate chain are unique to this

Client, and the Entity authenticates the Client using this unique certificate and/or using a

Resource Tag was included in the message received from the Entity to which this session is a

response (col. 11, line 5 – col. 12, line 20).

20.   For claim 15, Geiger teaches that said Entity comprises a Merchant.

21.   Claims 16-18 are drawn to a method that effectively describes the activities undertaken

by the hardware system as drawn in claim 2. It is well known in the art that the underlying

method of a given system is functionally equivalent to said system. Therefore, since claim 2 is

rejected, then claims 16-18 are also rejected for the reasons above. A teaching regarding the

method/system equivalence is available upon request.

22.   Claims 19 and 20 are drawn to the limitations in claim 15. Therefore, since claim 15 is

rejected, claims 19 and 20 are also rejected for the reasons above.

23.   Claim 22 is drawn to a software system that implements the method drawn in claim 16.

It is well known in the art that a system implementation is functionally equivalent to the

underlying method. Therefore, since claim 16 is rejected, claim 22 is also rejected for the

reasons above. A teaching that shows the functional equivalence will be included upon request.

Claim Rejections - 35 USC § 103

24.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

25.   Claims 5, 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Geiger as

applied to claims 1, 4 above, and further in view of Liao et al. (6,148,405).

26.   For claim 5, Geiger teaches a landline connection with a gateway to wireless networks

(Fig. 1, #18; col. 3, lines 49-51), but does not expressly disclose that the underlying landline

network connection is a TCP-based network connection. Liao teaches a method (abstract) of

securing communications through session key methods (col. 1, line 20 – col. 4, line 65) in which

the underlying network connection (Fig. 1, #104) is a TCP connection (col. 6, lines 18-21). At

the time the invention was made, one of ordinary skill in the art would have used a Liao landline-

wireless method in Geiger's system in order to use current networks while increasing

transmission efficiency (col. 2, line 65 – col. 3, line 10).

27.   For claim 8, Geiger teaches the use of third-party servers (col. 9, lines 29-67), but does

not expressly disclose that the matching destination address comprises a URL or URL based

address. Liao teaches this limitation (col. 12, line 46 – col. 13, line 52). At the time the

invention was made, one of ordinary skill in the art would have used a URL as a Geiger

matching destination address in order to facilitate the usage of third party service providers (col.

12, lines 46-53).

28.   Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Geiger as applied

to claim 2 above, and further in view of Herman et al. (6,341,353), Weber et al. (5,812,668) and

Nykanen et al. (6,714,778).

29.   For claim 10, Geiger teaches secured communications, but does not expressly disclose

that the secured web page is secured by any of SSL, PCT, or TLS. Herman teaches a method

(abstract) of web security (col. 1, line 10 – col. 2, line 42) using SSL security (col. 41, lines 20-40; col. 43, lines 1-30). Weber teaches a method (abstract) for providing security (col. 1, line 5 – col. 4, line 55) for which PCT is used (col. 3, line 40). Nykanen teaches a method (abstract) for private security (col. 1, line 5 – col. 2, line 20) that uses TLS (col. 7, lines 34-48; co0l. 13, lines 34-50). At the time the invention was made, one of ordinary skill in the art would have added these types of security to ensure security using common protocols (Herman, col. 1, lines 20-25).

30.   Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Geiger as applied to claim 2 above, and further in view of Micali (5,717,759).

31.   For claim 21, Geiger does not expressly disclose that the trusted source or storage means comprises a Compact Certificate or chain of Compact Certificates leading to a trusted public root key. Micali teaches a method (abstract) of utilizing public keys and digital signatures for communications setup (col. 1, line 10 – col. 4, line 45) in which compact certificates are used in the above manner (col. 5, lines 35-67). At the time the invention was made, one of ordinary skill in the art would have used compact certificates in Geiger in order to gain computation savings (col. 5, lines 15-35).

Conclusion

32.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Melvin H Pollack whose telephone number is (571) 272-3887. The examiner can normally be reached on 8:00-4:30 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Jack Harvey can be reached on (571) 272-3896. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

.system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MHP
23 November 2004

JACK B. HARVEY
SUPERVISORY PATENT EXAMINER